

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF :

CRIMINAL COMPLAINT AND ARREST
WARRANT FOR CHARLES ANTHONY
FORAME, IV

THE SEIZURE AND SEARCH OF A 2022
CHEVROLET TRAILBLAZER BEARING
VEHICLE IDENTIFICATION NUMBER
("VIN") KL79MPSL0NB026411

THE SEARCH OF THE PERSON OF
CHARLES ANTHONY FORAME, IV

Filed Under Seal

Case No. 1:24-mj-1269-CDA

Case No. 1:24-mj-1270-CDA

Case No. 1:24-mj-1271-CDA

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT, ARREST, and
SEARCH WARRANTS

I, Special Agent Leslie Adamczyk of the Federal Bureau of Investigation ("FBI"), being
duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for:

a. A criminal complaint charging **CHARLES ANTHONY FORAME, IV**
("**FORAME**") with 18 U.S.C. §2422(b) (enticement of a minor for the purposes of
engaging in illegal sexual activity), 18 U.S.C. § 2251(a) (production of child pornography),
18 U.S.C. § 2252A(a)(2) (receipt of child pornography), 18 U.S.C. § 2252A(a)(5)(B)
(possession of child pornography), and 18 U.S.C. § 1591 (sex trafficking of children).

b. a search warrant under Rule 41 of the Federal Rules of Criminal Procedure
to search 1) a 2022 Chevrolet Trailblazer bearing Maryland license tag 4EV5584 and
Vehicle Identification Number ("VIN") KL79MPSL0NB026411 (hereinafter, the

“**SUBJECT VEHICLE.**”) and 2) the person of Charles Anthony **FORAME** IV (together the “**SUBJECT LOCATIONS**”) further described in Attachments A-1 and A-2, for the items described in Attachment B.

2. Based on the facts set forth in this affidavit, there is probable cause to believe that Charles Anthony **FORAME**, IV has committed violations of 18 U.S.C. §2422(b) (enticement of a minor for the purposes of engaging in illegal sexual activity), 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), and 18 U.S.C. § 1591 (sex trafficking of children), among other federal criminal statutes (collectively the “**TARGET OFFENSES**”). I believe probable cause exists to search the **SUBJECT LOCATIONS** for evidence, fruits, and instrumentalities of the **TARGET OFFENSES** and to arrest **FORAME** for committing the **TARGET OFFENSES**.

AFFIANT BACKGROUND

3. I am a Special Agent with the FBI and have been since August 2012. I am currently assigned to the Maryland Child Exploitation and Human Trafficking Task Force in the Baltimore Division of the FBI and have been assigned investigations concerning sexual exploitation of children and child pornography. During my employment with the FBI, I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. In addition, I have also received training regarding the use of the Internet and digital communications as they pertain to federal investigations. I have participated in the execution of numerous search warrants, some of which have involved child exploitation offenses. Many of the search warrants resulted in the seizure of computers, cell phones and/or “smart phones,” magnetic storage media for computers, other electronic media, and other items evidencing violations of

federal laws. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts, and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts. I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7) who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Titles 18 and 21 of the United States Code.

4. I have set forth only the facts I believe are necessary to establish probable cause for the warrants sought herein. The information contained in this Affidavit is based upon my personal knowledge, my review of documents and official police reports, interviews with witnesses and other evidence and my conversations with other law enforcement officers and other individuals.

5. I know, based on my training and experience that DNA is found in human tissue and provides a genetic “blueprint” for each person. As such, DNA is unique to each person and it has accordingly been used by forensic scientists in a manner similar to fingerprints, that is, to identify persons who have left their DNA behind at crime scenes or on items of evidence. DNA evidence is extremely accurate as a means of identifying individuals; DNA can be found in any number of bodily tissues, including blood, hair, bone, and saliva.

6. I know, based on my training and experience, that items of evidentiary value, including but not limited to, DNA, fingerprints, blood, hair, saliva, clothing items, tools and/or items used in the commission of a crime are often left behind by both perpetrators and victims of crimes. This evidence is often left behind on clothing, upon vehicle surfaces, fabrics, and other mediums that the victim(s) and/or perpetrator(s) physically contact. Based on my training and

experience, many of these items of evidentiary value must normally be collected, examined, and analyzed by trained professionals before their relevance and ability to refute or corroborate other evidence may be realized.

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO
POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF
COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION,
RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY**

7. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure

and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

8. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children.

Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store,

maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

BRIEF OVERVIEW OF SNAPCHAT

9. Snapchat is owned by Snap, Inc. Snapchat is a messaging application for mobile devices. The application provides a way to share moments with photos, videos, and text. Some of the features of Snapchat are “Snaps,” “Stories,” “Memories,” and “Chat.” Snaps are when a

user takes a photo or video using their mobile device in real-time and selects which of their friends to send the message to. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender, and after the message is opened in the case of the recipient.) Users can save a photo or video locally to their device or to Memories, which is Snapchat's cloud-storage service.

10. A user can add photo or video Snaps to their "Story." Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all Snapchat users or just the user's friends for up to 24 hours. Stories can also be saved in Memories.

11. The Memories feature is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user. A user can also type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat application using the Chat feature. A user sends a Chat message to a friend and once it is viewed by both parties and both parties swipe away from the Chat screen, the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the Chat by tapping on the message that the user wants to keep. The user can clear the message by tapping it again.

PROBABLE CAUSE

12. On or about November 26, 2023, Complainant reported to the St. Mary's County Sheriff's Office that their daughter, Minor Victim 1¹, was in contact with an adult male using the Snapchat name Guccitrap4200 (hereafter "Guccitrap"). On or about November 27, 2023, Minor

¹ Minor Victim 1 was born in 2009 and was 14 years old in November 2023.

Victim 1 was forensically interviewed by the St. Mary's County Child Advocacy Center and stated the following:

- a. Minor Victim 1 was introduced to Guccitrap through Minor Witness 1, Minor Witness 2, and Minor Witness 3 (collectively the "Minor Witnesses"). The Minor Witnesses told Minor Victim 1 that if she met with Guccitrap and engaged in sexual activity with him, Guccitrap would give them things.
- b. Minor Victim 1 began talking with Guccitrap on Snapchat. During this conversation, Guccitrap told Minor Victim 1 "Let me fuck you and I'll take you guys wherever." Minor Victim 1 did not want to lose her virginity to him and so asked if she could give him oral sex.
- c. Minor Victim 1 gave Guccitrap her street address to pick her up. When Guccitrap was close, Minor Victim 1 told him she did not want to meet. He then stated he drove all this way and had her stuff. Minor Victim 1 decided to meet with him.
- d. After Guccitrap picked up Minor Victim 1, he drove to another street and pulled over. Guccitrap told Minor Victim 1 to get into the backseat, which she did, and he took off her clothes. Guccitrap then pushed Minor Victim 1's head down towards his penis to have her perform oral sex, while he touched the outside of her vagina with his hand. Guccitrap then pulled up Minor Victim 1, turned her around and attempted to insert his penis into her vagina. Minor Victim 1 pushed him off and told him no. Guccitrap then put lubricant on his penis and inserted it into her anus, ejaculating into a shirt which he took from a backpack in his car. After, Guccitrap gave Minor Victim 1 marijuana and THC cartridges (referred to as carts).

- e. Guccitrap attempted to meet with Minor Victim 1 again the following day and Minor Victim 1 blocked him on Snapchat.
 - f. Minor Victim 1 believed Guccitrap was 19 years old and later was told he was possibly 24 years old.
13. In their investigation, the St. Mary's County Sheriff's Office determined Guccitrap also used Snapchat name Guccitrap_hous3. In March 2024, the St. Mary's County Sheriff's Office contacted the FBI for assistance in identifying Guccitrap.
14. On or about April 04, 2024, Snapchat responded to an administrative subpoena with subscriber information for account Guccitrap_hous3. The verified phone number was listed as **443-545-6142 (SUBJECT TELEPHONE)** which was registered to Verizon from approximately July 2023 to December 2023 and T-Mobile from approximately December 2023 to present.
15. On or about April 10, 2024, Verizon responded to an administrative subpoena requesting subscriber information for **SUBJECT TELEPHONE**. The listed subscriber was Charles **FORAME** with an address of 1418 E Fort Ave, Baltimore, MD.
16. On or about April 04, 2024, T-Mobile responded to an administrative subpoena For subscriber information for **SUBJECT TELEPHONE**. The listed customer was Charles **FORAME**.
17. Maryland Motor Vehicle Administration records for **FORAME** show **FORAME** has a date of birth of 3/24/1994 and was issued his driver's license in 2022 with an address of 1418 E Fort Ave, Baltimore, MD 21230.
18. The St. Mary's County Sheriff's Office executed a search warrant on the Guccitrap4200 Snapchat account covering the time period of November 25, 2023 to November

27, 2023. Contained in the Snapchat search warrant return was an approximately five second video. In the video, a pubescent female is naked from the waist down and wearing a blue tie dye sweatshirt. She is sitting and her legs are spread, and she is rubbing her vagina with her hand. This video was sent to Guccitrap from an identified Snapchat account. The FBI determined the possible sender of the video was Minor Victim 2².

19. On or about April 22, 2024, Minor Victim 2 was forensically interviewed at the Anne Arundel County Child Advocacy Center and stated the following:

- a. Minor Victim 2 met Guccitrap on Snapchat. She initially stated he sent her an image of a gun and threatened her if she did not send him explicit photos/videos. Minor Victim 2 then stated he never sent her an image of a gun.
- b. Minor Victim 2 was shown screenshots from the video found in the search of Guccitrap's Snapchat account and identified herself in the screenshots. This video was taken in her bedroom, and she sent it to Guccitrap.

20. A review of conversations contained in the Snapchat search warrant return show Guccitrap communicated with Minor Victim 3³, Minor Victim 4⁴, and Minor Victim 5⁵.

21. During Minor Victim 1's first forensic interview in November 2023, the identity of Guccitrap was not known. On or about April 25, 2024, Minor Victim 1 was forensically interviewed by the FBI at the St. Mary's County Child Advocacy Center. Minor Victim 1 was shown an images of **FORAME**. Minor Victim 1 identified him as Guccitrip.

22. A review of the conversation between Guccitrap and Minor Victim 3, show they met in person and Minor Victim 3 left her cell phone in his car. They discuss him coming back to

2 Minor Victim 2 was born in 2010 and was 13 years old in November 2023.

3 Minor Victim 3 was born in 2007 and was 16 years old in November 2023.

4 Minor Victim 4 was born in 2008 and was 15 years old in November 2023.

5 Minor Victim 5 was born in 2008 and was 15 years old in November 2023.

give Minor Victim 3 her phone before her mom found out and talk about having sexual intercourse when he dropped off the phone. On or about April 25, 2024, Minor Victim 3 was forensically interviewed at the St. Mary's County Child Advocacy Center and stated the following:

- a. Minor Victim 3 has known Guccitrap for approximately six months and met him on Snapchat. Minor Victim 3 does not remember his real name. They talked often and he was very nice. Minor Victim 3 and Guccitrap were talking for about a month before they met in person.
- b. Minor Victim 3 was pregnant with Guccitrap's child. Guccitrap knew she was pregnant and wanted her to keep the baby. Minor Victim 3 had an abortion the week before the forensic interview.
- c. Minor Victim 3 likely got pregnant in Guccitrap's car. Guccitrap first picked Minor Victim 3 up in a white small four door car with black leather interior. He then picked Minor Victim 3 up in a black SUV with a black or grey interior. Minor Victim 3 took a couple videos when they were together. Their faces were not visible in the videos and his penis was visible. Guccitrap wanted the videos but when Minor Victim 3 tried to send them to his number they did not send.
- d. During the times they met, Minor Victim 3 and Guccitrap engaged in oral sex and vaginal sex. They met approximately five times.
- e. Guccitrap was described as a skinny white male with dark brown hair and short facial hair and he sometimes wore glasses. He had a tattoo on his forearm and another tattoo Minor Victim 3 could not remember.

- f. Minor Victim 3 was shown a copy of the Snapchat conversation with GucciTrap4200 and identified him as Guccitrap.
- g. Guccitrap told Minor Victim 3 he was 21 years old.
- h. Minor Victim 3 was shown an image of **FORAME** and identified him as Guccitrap.

23. Minor Victim 3's cellular phone was obtained by the FBI and consent to search her phone was given by Minor Victim 3's mother. A review of the phone showed the TextNow application. In the application, there was a text conversation with **(SUBJECT TELEPHONE)**.

The following are excerpts from the text conversation:

- a. On or about March 10, 2024:
 - Minor Victim 3 tries to send three videos which are not visible.
 - Minor Victim 3: "Heyy bby can you send the videos pls [wink kiss emoji]"
 - **SUBJECT TELEPHONE:** "Yes send yours to baby"...
 - Minor Victim 3: "Did they send? My phone trippin" Minor Victim 3 attempts to send one video which is not visible.
 - **SUBJECT TELEPHONE:** "No I haven't gotten any yet" "Did u get the ones I sent"
 - Minor Victim 3: "Noo..." "Send them to me on Instagram"
- b. On or about April 13, 2024:
 - Minor Victim 3: "I'm pregnant"
 - **SUBJECT TELEPHONE:** "You bein fr or?????"... "Do u think it is mine"...
- c. On or about April 20, 2024:
 - **SUBJECT TELEPHONE:** "Hey so what happened" "You didn't keep me updated baby"...
 - Minor Victim 3: "I had to I wish I could have kept it though [sad emoji face]"
- d. On or about April 21, 2024:
 - Minor Victim 3: "Ya it's kinda sad"

- **SUBJECT TELEPHONE:** “Wyd” “Wanna fuck”

24. A review of the Snapchat conversation between Guccitrap and Minor Victim 4 appeared to indicate they were making plans to meet in person when Minor Victim 4’s mother was at work. On or about April 29, 2024, Minor Victim 4 was forensically interviewed at the Charles County Child Advocacy Center. Minor Victim 4, who knew Guccitrap as “Charles,” stated the following:

- a. “Charles” added Minor Victim 4 on Snapchat a year or two ago. His username was Gucci something. He had multiple Snapchat accounts that were similar names including Gucci. Minor Victim 4 saw he was selling drugs and messaged him asking to buy a THC cartridge.
- b. Minor Victim 4 was shown an image of **FORAME** and identified him as “Charles.” Minor Victim 4 had seen the picture before on Charles’ Facebook.
- c. A year ago, “Charles” told Minor Victim 4 he had just graduated and was 19 or 20 years old. “Charles” knew Minor Victim 4 was in high school and was 15 years old.
- d. Minor Victim 4 identified Snapchat user Guccitrap4200 as “Charles.”
- e. Minor Victim 4 and “Charles” hung out for a while and he has come to Minor Victim 4’s mother’s apartment a couple times and Minor Victim 4 guessed there were things that happened that were not okay.
- f. “Charles” drove a blue four door SUV⁶. Minor Victim 4 described “Charles” as tall and skinny with dark hair. He had one tattoo of writing on his arm.

6 MVA records show a 2022 Chevrolet utility vehicle registered to FORAME. A search of the National Highway Traffic Safety Administration online VIN decoder show this vehicle is a Chevrolet Trailblazer.

25. A review of the Snapchat conversation between Guccitrap and Minor Victim 5 show Guccitrap offered to give Minor Victim 5 free stuff if they met for sex or if Minor Victim 5 sent him pictures and videos. Minor Victim 5 agrees to send Guccitrap images/videos for two nics⁷. Minor Victim 5 appears to send an image/video which was not visible in the search warrant return. Guccitrap says “Why’s it so dark?? I cant even see ya pussy”... “All I wanted was a decent video of u playing with that pussy”... “And if u do it with the light on and show that pussy good I’ll give u 3 of them instead”. Minor Victim 5 appears to send another image/video. This image/video was not returned in the search warrant return.

26. On or about May 14, 2024, Minor Victim 5 was forensically interviewed at the Georgetown, Delaware Child Advocacy Center. Minor Victim 5 stated the following:

- a. Minor Victim 5 met Guccitrap on Snapchat sometime around November 2023.
- b. Minor Victim 5 was shown Snapchat messages between her and Guccitrap and identified her Snapchat account.
- c. Minor Victim 5 stated Guccitrap offered her “nics” in exchange for videos.
- d. Minor Victim 5 stated she made and sent a video for Guccitrap. In the video she showed her breasts and vagina.
- e. Minor Victim 5 did not meet up with Guccitrap and never received any of the nicotine/THC cartridges Guccitrap promised.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for contraband, evidence, fruits, and instrumentalities of the **SUBJECT OFFENSES** that

⁷ “Nic” is likely referring to nicotine vapes.

might be found at the **SUBJECT LOCATIONS**, in whatever form they are found. One form in which the evidence might be found is as records in the form of data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of computers and storage media and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable cause.* I submit that if a computer or storage medium is found on the **SUBJECT LOCATIONS**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers

were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT LOCATIONS** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations; computer activity associated with user accounts; electronic storage media that connected with the computer; and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to access with intent to view, possess, distribute, or receive child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence

of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, and/or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

32. This warrant permits law enforcement to compel **FORAME** to unlock any and all devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices (like smartphones) and laptops, offer their users the ability to unlock the device through biometric

features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your affiant has reason to believe that one or

more digital devices will be found during the search. Additionally, based on my training and experience, individuals can access their social media accounts through multiple electronic platforms, to include cellular phones. Snapchat, the social media used by **FORAME**, offers mobile apps for use in iOS or Android. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the **DEVICES**, making the use of biometric features necessary to the execution of the search authorized by this warrant.

- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **FORAME** to the fingerprint scanner of the devices found at the **SUBJECT LOCATIONS**; (2) hold the devices found at the **SUBJECT LOCATIONS** in front of the face of **FORAME** and activate the facial recognition feature; and/or (3) hold the devices found at the **SUBJECT LOCATIONS** in front of the face of **FORAME** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that **FORAME** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to ask **FORAME** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

AUTHORIZATION REQUEST

33. Based on the foregoing information, there is probable cause to believe that **CHARLES ANTHONY FORAME, IV**, violated 18 U.S.C. § 2242 (b) (enticement of a minor for the purposes of engaging in illegal sexual activity), U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), and 18 U.S.C. § 1591 (sex trafficking of children). Specifically beginning on or about November 1, 2023 through May 1, 2024, FORAME used a facility of interstate commerce to knowingly persuade, induced, entice or coerce minors to engage in prostitution and engage in any sexual activity for which a person can be charge; and FORAME knowingly employed, used, persuaded, induced, enticed, or coerced minors to engage in sexual explicit conduct for the purpose of producing a visual depiction of such conduct knowing the visual depicting would be transported in interstate commerce; and FORAME knowing received and possessed child pornography knowing it was transported in and affecting interstate commerce; and FORAME recruited, enticed, transported and solicited minor by any means to engage in a commercial sex act.

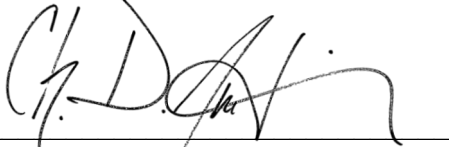
34. Based on the above information, I respectfully submit that there is probable cause to believe that evidence, fruits, or instrumentalities of the **TARGET OFFENSES** are within the **SUBJECT LOCATIONS**. I request that the Court issue the proposed search warrants, pursuant to Federal Rule of Criminal Procedure 41. The property to be seized is described in Attachment A-1 and Attachment A-2. I therefore respectfully request that a search warrant be issued authorizing a search of the **SUBJECT LOCATIONS** for items described above and in Attachment B and authorizing the seizure and examination of any such items found therein

S//Leslie Adamczyk

Leslie Adamczyk
Special Agent, FBI

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with

Fed. R. Crim. P 4.1 and 41(d)(3) this 23rd day of May, 2024.

A handwritten signature in black ink, appearing to read 'C.D. Austin', written over a horizontal line.

The Honorable Charles D. Austin
United States Magistrate Judge
District of Maryland